UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/722,822	11/25/2003	Amit Raikar	200309668-1	9372

22879 7590 09/02/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
09/02/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte AMIT RAIKAR

Appeal 2009-007105
Application 10/722,822
Technology Center 2400

Before ROBERT E. NAPPI, JOHN C. MARTIN,
and ELENI MANTIS MERCADER, *Administrative Patent Judges*.

MANTIS MERCADER, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the non-final rejection of claims 1-26. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

INVENTION

Appellant's Figure 3 is reproduced below:

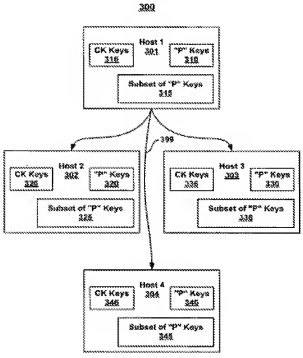

FIG. 3

Appellant's Figure 3 depicts a group-based communication 300 for dynamic source authentication having communication group member hosts 301, 302, 303, and 304 (Spec. 10:1-5).

Appellant's claimed invention is directed to a group-based communications environment 300 allowing a group host, such as host 301, to multicast a message 399 to all members of the group, such as hosts 302,

303, and 304, at one time. Each host is distributed a set of "P" keys for generating message authentication codes (MACs) attached to outgoing messages, where "P" is the number of keys. The sender of a message to the group attaches "P" MACs to the outgoing message. The MACs are hashes on the packet message data created with each of the "P" keys. No two hosts use the same set of sender keys (e.g., "P" keys) to encrypt an outgoing message.

Each receiver in the group is distributed a subset of the "P" keys with which it verifies authenticity of a subset of the MACs (e.g., according to the key the receiver holds), while the rest of the MACs can be assumed to be correctly authenticated. For example, host 301 comprises subset keys 315.

In addition to the "P" keys and the subset of "P" keys, each host of the group is distributed a set of complementary keys (e.g., CK keys). For example, host 301 comprises CK keys 316. The CK keys are used for key revocation when, for example, a host is added or removed from the group. *See* Spec. 10-11.

Claim 1, reproduced below, is representative of the subject matter on appeal:

1. A method for establishing secure group-based communication comprising:

distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts; and

distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

THE REJECTION

The Examiner relies upon the following as evidence of unpatentability:

Sowa US 2002/0154776 A1 Oct. 24, 2002

The following rejection is before us for review:

The Examiner rejected claims 1-26 under 35 U.S.C. § 102(b) as being anticipated by Sowa.

ISSUE

The pivotal issue is whether Sowa teaches the limitations of: "group-based communication" and "dynamically modifying" a set of first keys, as recited in representative claim 1.

FINDINGS OF FACT (FF)

The following Findings of Fact are supported by a preponderance of the evidence:

1. Sowa teaches that the "Common Cipher Key (CCK) is a group key" in the sense that multiple mobile stations (MSs) have the same CCK (¶ [0044]).
2. Sowa also teaches that while the CCK has no relation to a particular talkgroup (TG), the CCK is geographically specific, i.e., the CCK serves all units within a given location area (¶ [0044]).
3. Sowa teaches that that the CCK is a location based traffic key meant for use with the encryption of *group call traffic* (¶ [0101]).
4. Sowa teaches that there could be more than one location having the same CCK (¶ [0101]).
5. Sowa explicitly teaches that a CCK is identified by CCK-ID, and through gradual rekeying, "[a] *new CCK replaces the oldest CCK-ID*" (¶ [0101] (emphasis added)).

6. Appellant's Specification defines "modifying the sets of keys" as "[r]e-keying" the keys (Spec. 17:12-17).

PRINCIPLES OF LAW

"During examination, 'claims . . . are to be given their broadest reasonable interpretation consistent with the specification, and . . . claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art.'" *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citation omitted); *In re Morris*, 127 F.3d 1048, 1053-54 (Fed. Cir. 1997). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (citation omitted).

ANALYSIS

Analysis regarding the limitation of a "group-based communication"

Appellant argues (Br. 10) that, contrary to the Examiner's interpretation of Sowa's paragraph [0044], Sowa teaches that "'the CCK has no relation to a particular talk group (TG).'" Appellant further argues (Br. 10) that a geographic location does not define a group because Sowa specifically states that the CCK has no relation to a talk group. Appellant also argues (Br. 10) that because Sowa's paragraph [0101] states that "it is possible for more than one location area to have the same CCK," a geographic location can not be considered a communication group when a different location can have the same CCK.

We are not persuaded by Appellant's arguments. Sowa teaches that the "*Common Cipher Key (CCK) is a group key*" in the sense that multiple MSs have the same CCK (FF 1). Sowa also teaches that while the CCK has no relation to a particular TG, the CCK is geographically specific, i.e., the CCK serves all units within a given location area (FF 2). Furthermore, Sowa teaches that that the CCK is a location based traffic key meant for use with the encryption of *group call traffic* (FF 3). Accordingly, Sowa teaches a group key CCK which serves all members of a communication group in a geographic location. Notice that the claim language does not recite a specific type of a group such as a "talkgroup," and thus, any communication group (e.g., a location based communication group) would be sufficient to meet the limitation of a "group-based communication" as recited in representative claim 1.

We are also not persuaded by Appellant's argument (Br. 10) regarding multiple locations having the same CCK (*see also* FF 4), because multiple locations, as opposed to a single location, just indicates the size of the group, which may be enlarged to include group members from multiple locations. Just because the size of the group is bigger, it does not mean it is not a group.

Analysis regarding the limitation of a "dynamically modifying" a first set of keys

Appellant further argues (Br. 11) that Sowa's paragraph [0045] does not teach "dynamically modifying said first set of keys," because Sowa teaches that "a GCK is defined for each talk group in the system," and thus, Sowa does not dynamically modify the CCK (e.g., the first set of keys) because the CCK has "no relation to a particular talk group."

We are not persuaded by Appellant's argument, and we agree with the Examiner's reference to Sowa's Figure 14 (Ans. 7), because Sowa explicitly teaches that a CCK is identified by CCK-ID, and through gradual rekeying, "[a] *new CCK replaces the oldest CCK-ID*" (FF 5). Note that Appellant's Specification describes "modifying the sets of keys" by "[r]e-keying" the keys (FF 6). Accordingly, Sowa does teach "dynamically modifying" a CCK having a CCK-ID by rekeying a new CCK, based on the broadest reasonable interpretation in view of Appellant's Specification. *See Phillips*, 415 F.3d at 1315.

Accordingly, we will affirm the Examiner's rejection of representative claim 1, and for similar reasons, we will affirm the rejections of claims 2-26.

CONCLUSION

Sowa teaches the limitations of: "group-based communication" and "dynamically modifying" a set of first keys.

ORDER

The decision of the Examiner to reject claims 1-26 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED

babc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528